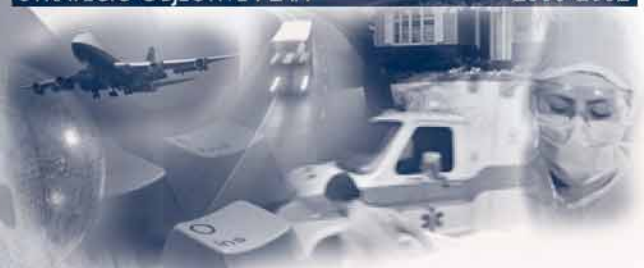
GAO

Accountability * Integrity * Reliability

Serving the Congress and the Nation

Diffuse Security Threats

Strategic Objective Plan 2000-2002



GAO's Mission

GAO exists to support the Congress in meeting its Constitutional responsibilities and to help improve the performance and accountability of the federal government for the benefit of the American people.

Core Values

Accountability

describes the nature of GAO's work. GAO helps the Congress oversee federal programs and operations to ensure accountability to the American people. GAO's evaluators, auditors, lawyers, economists, public policy analysts, information technology specialists, and other multidisciplinary professionals seek to enhance the economy, efficiency, effectiveness, and credibility of the federal government both in fact and in the eyes of the American people. GAO accomplishes its mission through a variety of activities, including financial audits, program reviews, investigations, legal support, and program analyses.

Integrity

describes the high standards that GAO sets for itself in the conduct of its work. GAO takes a professional, objective, fact-based, nonpartisan, nonideological, fair, and balanced approach to all of its activities. Integrity is the foundation of reputation, and GAO's approach to its work ensures both.

Reliability

describes GAO's goal for how its work is viewed by the Congress and the American public. GAO produces high-quality reports, testimony, briefings, legal opinions, and other products and services that are timely, accurate, useful, clear, and candid.

FOREWORD

In fulfilling its mission, GAO examines the use of public funds; evaluates federal programs and activities; and provides analyses, options, recommendations, and other assistance to help the Congress make effective oversight, policy, and funding decisions. In this context, GAO works to continuously improve the economy, efficiency, and effectiveness of the federal government through the conduct of financial audits, program reviews and evaluations, analyses, legal opinions, investigations, and other services. Most of this work is based upon original data collection and analysis.

To ensure that GAO, in serving the Congress, targets the right issues, provides balanced perspectives, and develops practical recommendations, GAO regularly consults with the Congress and maintains relationships with a variety of federal, state, academic, and professional organizations. GAO also obtains the perspectives of applicable trade groups and associations and attends professional conferences. Moreover, GAO regularly coordinates its work with CRS, CBO, and agency Inspector General offices. Throughout, GAO's core values of accountability, integrity, and reliability are guiding principles.

In keeping with its mission and responsibilities, GAO has developed a strategic plan that includes four strategic goals and 21 related strategic objectives. To ensure that GAO's resources are directed to achieving its goals, a separate strategic plan underlies each objective. In support of GAO's goal of providing timely, quality service to the Congress and the federal government to respond to changing security threats and the challenges of global interdependence, this strategic plan describes the performance goals GAO will use in supporting congressional and federal decisionmaking on U.S. preparedness to respond to diffuse threats to national and global security.

This plan covers a 3-year period; however, because unanticipated events may significantly affect even the best of plans, GAO's process allows for updating this plan to respond quickly to emerging issues. If you have questions or desire information on additional or completed work related to this strategic objective, please call or e-mail us or the contact persons listed on the following pages.

Henry L. Hinton, Jr.
Assistant Comptroller General
National Security and International Affairs Division
(202) 512-4300
hintonh.nsiad@gao.gov

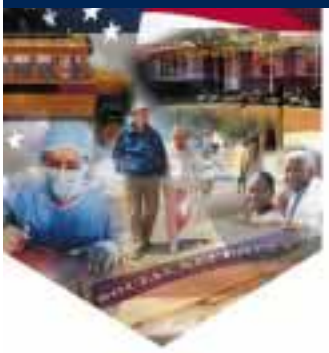
Keith O. Fultz
Assistant Comptroller General
Resources, Community, and Economic Development Division
(202) 512-3200
fultzk.rced@gao.gov

Serving the Congress
GAO's Strategic Plan Framework

Mission

GAO exists to support the Congress in meeting its Constitutional responsibilities and to help improve the performance and accountability of the federal government for the benefit of the American people.

Goals

Provide Timely, Quality Service to the Congress and the Federal Government		Support the Transition	Maximize the Value of GAO
			
to Address Current and Emerging Challenges to the Well-Being and Financial Security of the American People	to Respond to Changing Security Threats and the Challenges of Global Interdependence	to a More Results-Oriented and Accountable Federal Government	by Being a Model Organization for the Federal Government

Themes

Demographics | **Globalization** | **Quality of Life** | **Security** | **Technology**

Government Performance and Accountability

Objectives

- Health care needs and financing
- Retirement income security
- Social safety net
- Education/workforce issues
- Effective system of justice
- Community investment
- Natural resources use and environmental protection
- Physical infrastructure

DIFFUSE SECURITY THREATS

- Military capabilities and readiness
- Advancement of U.S. interests
- Global market forces

- Fiscal position of the government
- Government financing and accountability
- Governmentwide management reforms
- Economy, efficiency, and effectiveness improvements in federal agencies

- Client relations
- Strategic and annual planning
- Human capital
- Core business and supporting processes
- Information technology services

Core Values

Accountability | **Integrity** | **Reliability**

Provide Timely, Quality Service to the Congress and the Federal Government

to Respond to Changing Security Threats and the Challenges of Global Interdependence

DIFFUSE SECURITY THREATS

Military capabilities and readiness

Advancement of U.S. interests

Global market forces

Responding to Diffuse Threats to National and Global Security

The United States faces threats to its security and economy from new sources. The bombings of the World Trade Center in New York City in 1993 and the federal building in Oklahoma City in 1995, along with the use of a nerve agent in the Tokyo subway in 1995, have elevated concerns about terrorism in the United States. Likewise, the bombings of the Khobar Towers in Saudi Arabia in 1996 and the U.S. Embassies in Kenya and Tanzania in 1998 have heightened concerns about the safety of U.S. military installations and diplomatic missions overseas.

At least nine countries posing national security concerns are believed to have weapons of mass destruction (nuclear, biological, and chemical weapons). The number is expected to grow. Since 1991, the Departments of Defense, Energy, and State have been authorized to spend $4.7 billion to prevent the further spread of such weapons.

Protection of the nation's critical infrastructure, including energy, financial service, and transportation systems, is becoming increasingly important largely because of their dependence on complex interconnected computer systems. Criminals, terrorists, and others, working anonymously from remote locations and with relatively limited resources, can now use computers and the open interconnectivity of the Internet to severely disrupt this infrastructure, which is essential to our national defense, economic prosperity, and quality of life. Presidential Decision Directive 63, issued in May 1998, prompted an array of federal activities aimed at improving the protection of critical infrastructure, especially enhancing information security, in both the private and public sectors.

GAO's strategic plan identifies five multiyear performance goals to support congressional and federal decisionmaking on responding to diffuse threats to national and global security. (Because the activities of the intelligence community are overseen by the House and Senate Select Committees on Intelligence, they are not addressed in this plan.) The following pages discuss the significance of the performance goals, the key efforts that will be undertaken, and the potential outcomes.

Performance Goals

- Analyze the Effectiveness of Federal Agencies' Programs to Combat Terrorism
- Assess the Effectiveness of U.S. Programs and Agreements to Prevent the Proliferation of Nuclear, Biological, and Chemical Weapons
- Assess U.S. Efforts to Protect Computer–Supported Critical Infrastructure for Business and Government
- Assess DOD's Ability to Retain Information Superiority on the Battlefield
- Assess the Effectiveness of the Department of Transportation's Oversight of Domestic and International Aviation Security

Analyze the Effectiveness of Federal Agencies' Programs to Combat Terrorism

Significance

Combating terrorism at home and abroad is a high-priority national security and law enforcement concern. The terrorism threat to U.S. security has led to major initiatives by the administration and the Congress. More than 40 federal agencies, offices, and bureaus spend over $10 billion a year to combat domestic and international terrorism. In addition, the President has requested $3 billion over the next 5 years for embassy security. The many and increasing number of participants and programs in the terrorism area across the federal government pose a difficult management and coordination challenge to avoid program duplication, fragmentation, and gaps.

Presidential Decision Directive 63, issued in May 1998, mandated the preparation of a National Plan for Critical Infrastructure Protection. The plan, expected to be issued in late 1999 by the Critical Infrastructure Office in the Department of Commerce, is to summarize a national strategy for protecting our critical infrastructure (such as that for telecommunications, transportation, power distribution, and financial services) from hostile attacks that could cause devastating disruptions. Such attacks could be physical (e.g., bombs or biological or chemical agents) or electronic (hacker-type) on the computers that provide essential support to most of our nation's critical infrastructure.

Key Efforts	*Potential Outcomes*
Review best practices of foreign governments in counterterrorism programs	Identify options to improve agencies' mission definition, better prioritize funding and programs, and improve program management
Examine potential duplication in the training of first responders (those providing fire, police, and emergency medical services) for dealing with weapons of mass destruction	Reduction of unnecessary duplication among federal agencies' capabilities to respond to, prepare for, and manage the consequences of a chemical, biological, radiological, or nuclear terrorist incident
Assess potential overlap in federal capabilities to respond to and manage the consequences of weapons of mass destruction and terrorist incidents	
Assess efforts to enhance security of personnel and property at U.S. embassies and consulates	Improved accountability for, and more effective use of, the multibillion-dollar fund for the embassy security program
Evaluate the adequacy of the National Plan for Critical Infrastructure Protection	Improved plan for protection of the nation's critical infrastructure
Assess the efforts of federal law enforcement agencies to prevent, detect, and respond to terrorist events	More efficient and effective use of resources to deter, detect, and respond to terrorist crimes and minimize collateral damage
Evaluate the adequacy of the Department of Health and Human Services' Bioterrorism Initiative	

CONTACTS FOR ADDITIONAL INFORMATION: Norman J. Rabkin, Director, National Security Preparedness Issues, (202) 512-5140, rabkinn.nsiad@gao.gov; Benjamin F. Nelson, Director, International Relations and Trade Issues, (202) 512-4128, nelsonb.nsiad@gao.gov; Laurie Ekstrand, Director, Administration of Justice Issues, (202) 512-2758, ekstrandl.ggd@gao.gov; Jack L. Brock, Director, Governmentwide and Defense Information Systems, (202) 512-6240, brockj.aimd@gao.gov

Assess the Effectiveness of U.S. Programs and Agreements to Prevent the Proliferation of Nuclear, Biological, and Chemical Weapons

Significance

The continuing proliferation of weapons of mass destruction and delivery systems poses serious threats to the security of the United States. The danger that in the near future a rogue regime will be able to threaten the United States or its allies with ballistic missiles armed with nuclear, chemical, or biological warheads has led the United States to initiate a variety of programs aimed at preventing such an outcome. For example, DOD's Cooperative Threat Reduction Program is now the centerpiece of a growing multibillion-dollar array of DOD's, DOE's, and the State Department's efforts to help former Soviet states control and reduce their vast, diverse holdings of Cold War-era nuclear, chemical, and biological weapons and delivery systems and related infrastructure. These efforts must overcome numerous obstacles in the former Soviet states, including a precipitous decline in Russia's economy that has led the United States to assume an increasing share of the cost of controlling former Soviet weapons of mass destruction. U.S. efforts must therefore focus on the former Soviet assets that pose the greatest risks and effectively reduce those risks. The United States is also seeking to ensure that it does not contribute to the proliferation of weapons of mass destruction through the careless handling of materials and classified data at U.S. nuclear and other weapons facilities. In addition, the United States controls exports of certain sensitive technologies (such as high-performance computers) and has entered into several export control agreements with other nations capable of supplying sensitive technologies. However, such controls can be weakened by the pace of technological change and by efforts by countries of concern to circumvent export controls.

Key Efforts	*Potential Outcomes*
Evaluate the effectiveness and management of executive branch efforts to minimize the proliferation of former Soviet nuclear, chemical, and biological assets that pose the greatest risk to the United States	Improved management of programs and increased focus on former Soviet biological weapons institutes that pose the greatest risks to U.S. national security
Review the adequacy of DOE's actions to improve security controls at the U.S. nuclear weapons complex	Enhanced controls aimed at preventing the theft of U.S. nuclear expertise by other countries
Assess the effectiveness of U.S. controls over the exports of goods and technologies that could facilitate proliferators' efforts to develop weapons of mass destruction	Enhanced controls over the export of U.S. technologies that could facilitate the proliferation of weapons of mass destruction

CONTACTS FOR ADDITIONAL INFORMATION: Benjamin F. Nelson, Director, International Relations and Trade Issues, (202) 512-4128, nelsonb.nsiad@gao.gov; Jim Wells, Director, Energy, Resources, and Science Issues, (202) 512-3841, wellsj.rced@gao.gov

Assess U.S. Efforts to Protect Computer-Supported Critical Infrastructure for Business and Government

Significance

Protection of the nation's critical infrastructure—including that for energy, financial services, transportation, vital human services, and communications systems—from cyber attacks is becoming increasingly important due largely to the dependence of infrastructure on complex interconnected computer systems. Criminals, terrorists, and others, working anonymously from remote locations and with relatively limited resources, can now use computers to severely disrupt the infrastructure systems that are essential to our national defense, economic prosperity, and quality of life. Similar means can be used to commit massive fraud and gain access to highly sensitive information. In response, Presidential Decision Directive 63, which was issued in May 1998, and the National Plan for Information Sytems Protection, which was issued in January 2000, have prompted an array of federal activities aimed at improving the protection of critical infrastructure, especially enhancing information security, in both the public and private sectors.

Key Efforts	*Potential Outcomes*
Assess computer security controls associated with critical federal systems	Reasonable assurance that critical operations are protected from disruption, fraud, and misuse
Evaluate computer security processes of unique or high-risk federal government applications, such as Social Security	Enhanced capability of organizations to detect, protect against, and respond to computer intrusions
Assess federal efforts to establish and promote public-private partnerships to reduce the threat of cyber attacks	Greater coordination among public- and private-sector institutions in protecting U.S. computer-based critical infrastructure systems
Provide assistance to the Congress in identifying potential changes to computer security legislation	Improvements to the legislative framework for information security
Assess the government's efforts to limit fraudulent activity such as credit card fraud over the Internet	Greater public assurance that Internet and electronic commerce transactions are secure
Evaluate federal efforts to facilitate development of standards for communications among computers over the Internet to make it easier to conduct electronic government	More secure and efficient electronic government operations

CONTACT FOR ADDITIONAL INFORMATION: Jack L. Brock, Director, Governmentwide and Defense Information Systems, (202) 512-6240, brockj.aimd@gao.gov

Assess DOD's Ability to Retain Information Superiority on the Battlefield

Significance

DOD and the services are investing billions of dollars to attain information superiority, with the expectation that this investment will result in more effective operations by U.S. and allied forces. Information superiority is expected to result in increased survivability of the forces and the improved ability of the forces to accomplish their mission objectives sooner. Whether DOD and the services can attain that information superiority will depend on how well they select and manage their own related research, development, and acquisition efforts; how well they coordinate their efforts to consider interservice and U.S. allies' interoperability; and how well they test and develop their information superiority systems and networks to ensure protection against enemy attacks designed to disrupt them. At risk are not only the funds DOD and the services are investing but also future forces and missions.

Key Efforts	*Potential Outcomes*
Evaluate the Army's development, test, and acquisition plans for its Priority Two systems, which constitute the second tier of systems most important to the Army's efforts to digitize the battlefield	More effective funding, testing, and coordination of system developments to attain information superiority with the operational systems that are deployed
Evaluate the Army's Land Warrior development program, which is to significantly improve the destructive power, mobility, survivability, command and control, and sustainability of infantry soldiers by integrating a variety of components and technologies	Consideration by DOD and congressional committees of information and analysis of whether funds are being spent efficiently and wisely
Evaluate the Army's Warfighter Rapid Acquisition Program efforts, which are to speed up the fielding of urgently needed new technologies to soldiers	Consideration by DOD and congressional committees of information and recommendations to help ensure that accelerated acquisitions are justified and well managed
Evaluate the Navy's development, test, and acquisition plans to ensure the systems and networks that are to provide Navy-wide information communications for the 21st century will not be degraded by enemy efforts to interrupt them	Consideration by DOD and congressional committees of information and recommendations to help ensure that DOD and the services develop information systems and networks that operate without enemy interruption under wartime conditions
Evaluate DOD's Electronic Warfare Systems to determine if DOD is developing and maintaining systems that can jam, counterjam, or deceive an adversary's, radars, communications systems, or other sensor systems	Contribute to DOD's ability to better control the radio frequency spectrum on and over the battlefield to ensure information dominance
Evaluate DOD's Intelligence, Surveillance, and Reconnaissance Systems to determine if DOD is developing and maintaining systems that send the results to the warfighters in nearly real time	Better integration of DOD's intelligence systems with its command and control networks and weapons delivery systems

CONTACT FOR ADDITIONAL INFORMATION: Louis J. Rodrigues, Director, Defense Acquisition Issues, (202) 512-4199, rodriguesx.nsiad@gao.gov

Assess the Effectiveness of the Department of Transportation's Oversight of Domestic and International Aviation Security

Significance

The effectiveness of aviation security is crucial to ensuring the continued public confidence in the safety of air travel. The loss of 270 lives in the terrorist bombing of Pan Am Flight 103 over Lockerbie, Scotland, and terrorist bombings in the United States and abroad serve as reminders of the continuing threat of terrorism. Consequently, technology and human vigilance must keep pace with the increasing sophistication of bombs and other terrorist devices. In addition, other threats such as domestic extremist groups and "air rage" pose new problems for the security of commercial aviation. Within the Department of Transportation, the Federal Aviation Administration is responsible for protecting the users of commercial air transportation against terrorist and other criminal acts.

Key Efforts

Assess FAA's efforts to foster research and develop better explosives-detection technology and procedures

Assess FAA's efforts to identify and address key vulnerabilities in the security of U.S. commercial aviation

Assess FAA's management and integration of its research and development efforts at its Technical Center with FAA's overall aviation security efforts

Potential Outcomes

More effective approaches for developing, deploying, and using advanced security equipment and procedures

Better focus and prioritization of DOT's efforts to improve security measures and reduce vulnerabilities in the aviation system

Greater integration and use of aviation security research and development efforts

CONTACT FOR ADDITIONAL INFORMATION: John H. Anderson, Jr., Director, Transportation Issues, (202) 512-2834, andersonj.rced@gao.gov

The full set of GAO's strategic planning, performance, and accountability documents are listed below. All of these documents, as well as other GAO reports and documents, may be obtained electronically on our website, ***www.gao.gov.***


Accountability Report for fiscal year 1999

Strategic Plan, 2000-2005

Strategic Plan Executive Summary

Strategic Plan Framework

Strategic Objective Plans

Health Care Needs and Financing

Retirement Income Security

Social Safety Net

Education/Workforce Issues

Effective System of Justice

Community Investment

Natural Resources Use and Environmental Protection

Physical Infrastructure

Diffuse Security Threats

Military Capabilities and Readiness

Advancement of U.S. Interests

Global Market Forces

Fiscal Position of the Government

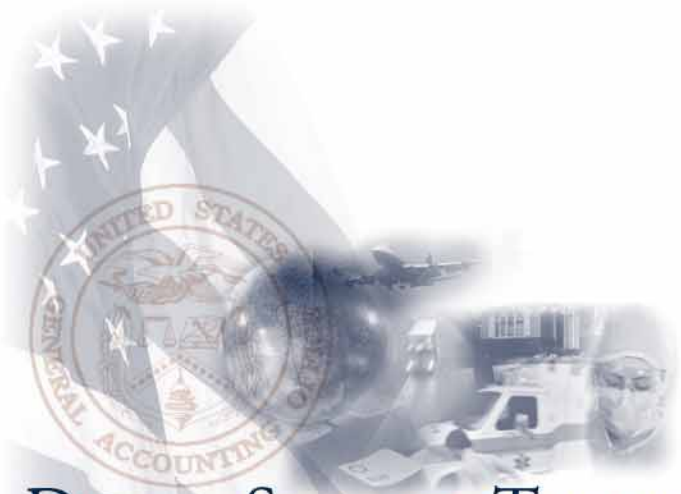
Government Financing and Accountability

Governmentwide Management Reforms

Economy, Efficiency, and Effectiveness Improvements in Federal Agencies

Maximize the Value of GAO

Performance Plan Fiscal Year 2001



DIFFUSE SECURITY THREATS

STRATEGIC OBJECTIVE PLAN 2000-2002